# IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

## Patent Application

**Appellant(s):** Garay et al.
**Case:** Garay 10-1 (LCNT/125336)
**Serial No.:** 10/611,771 **Group Art Unit:** 2136
**Filed:** June 30, 2003 **Confirmation #:** 2190
**Examiner:** Johnson, Carlton
**Title:** METHOD AND SYSTEM FOR FAIR EXCHANGE OF USER INFORMATION

**MAIL STOP APPEAL BRIEF-PATENTS**
**COMMISSIONER FOR PATENTS**
**P.O. BOX 1450**
**ALEXANDRIA, VA 22313-1450**

**SIR:**

## APPEAL BRIEF

Appellants submit this Appeal Brief to the Board of Patent Appeals and Interferences on appeal from the decision of the Examiner of Group Art Unit 2136 mailed July 26, 2007 finally rejecting claims 1, 3, 4, 6, 7, 9, 10, and 23-25.

In the event that an extension of time is required for this appeal brief to be considered timely ($120 one month extension), and a petition therefor does not otherwise accompany this appeal brief, any necessary extension of time is hereby petitioned for.

The Commissioner is authorized to charge the Appeal Brief fee ($510) and any other fees due to make this filing timely and complete (including extension of time fees) to Deposit Account No. 20-0782/LCNT/125336.

## Table of Contents

## Real Party in Interest

The real party in interest is LUCENT TECHNOLOGIES INC.

## Related Appeals and Interferences

Appellants assert that no appeals or interferences are known to Appellants, Appellants' legal representative, or assignee which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

## Status of Claims

Claims 1, 3, 4, 6, 7, 9, 10, and 23-25 are pending in the application. Claims 1-29 were originally presented in the application. Claims 1, 3, 4, 6, 7, 9, 10, 23-25 were amended. Claims 2, 5, 8, 11-22, and 26-29 were canceled. Claims 1, 3, 4, 6, 7, 9, 10, and 23-25 stand finally rejected as discussed below. The final rejection of claims 1, 3, 4, 6, 7, 9, 10, and 23-25 is appealed.

## Status of Amendments

All claim amendments have been entered.

## Summary of Claimed Subject Matter

Embodiments of the present invention are generally directed to providing a fair exchange of users' hidden values through a series of exchanges leading to completing these hidden values. In one embodiment, the invention includes a method of fairly exchanging a hidden value of a first user for a hidden value of a second user, by a series of exchanges between the first user and the second user, leading to completing each of the hidden values. A modulus and a modular function known to both users are established. The modular function iteratively produces a plurality of sequence values in such a way that each sequence value is related to the previous sequence value according to the modular function, thus conformance to the modulation function can be determined for adjacent sequence values. The total number of iterations over which the sequence values between the users will be exchanged is established. The sequence values of each user are iteratively exchanged between the users progressing in a predetermined order toward an end of the sequence values. The exchange is completed if the total number of iterations are completed. The exchange is terminated if the total number of iterations are not completed. In one embodiment, the hidden values are values immediately preceding the last values of the sequence values. In another embodiment the total number of iterations is at least 80.

For the convenience of the Board of Patent Appeals and Interferences, Appellants' independent claims 1 and 23 are presented below with citations to various figures and appropriate citations to at least one portion of the specification for elements of the appealed claims.

Claim 1 positively recites (with references to Appellants' specification and figures included in parentheses):

> 1. (previously presented) A method fairly exchanging a hidden value (320) of a first user for a hidden value (320) of a second user, by a series of exchanges (485) between the first user and the second user leading up to completing said hidden values, comprising the steps of:

establishing (Para. [0036]) a modulus and a modular function known to the first user and known to the second user, said modular function iteratively producing a plurality of sequence values (300) wherein each said sequence value is related, according to said modular function, to a next previous sequence value, whereby conformance to the modulation function can be determined for adjacent ones of the plurality of sequence values;

establishing (410) a total number of iterations over which the sequence values will be exchanged between the first user and the second user;

iteratively exchanging (485) the sequence values of the first and second users, progressing in a predetermined order toward an end of said sequence values (330);

completing (480/483) the exchange provided that the total number of iterations are completed, and terminating (480/490) the exchange if the total number of iterations are not completed.

Support for the elements of claim 1 can be found at least from the following sections of Appellants' specification: Paragraphs [0033]-[0036], [0039], [0044]-[0049], [0057]-[0066] and Figures 3, 4, and 6.

Claim 23 positively recites (with references to Appellants' specification and figures included in parentheses):

23. (previously presented) A system (500) for exchanging user information over a network (550/570) comprising:

at least one programmed processor (520) coupled to a memory (530) and arranged for conducting a fair exchange of a hidden value (320) of a first user for a hidden value (320) of a second user, by a series of exchanges between the first user and the second user leading up to completing said hidden values ;

establishing (Para. [0036]) a modulus and a modular function known to the first user and known to the second user, said modular function iteratively producing a plurality of sequence values (300) wherein each said sequence value is related, according to said modular function, to a next previous sequence value,

whereby conformance to the modular function can be determined for adjacent ones of the plurality of sequence values;

establishing (410) a total number of iterations over which the sequence values will be exchanged between the first user and the second user,

iteratively exchanging (485) the sequence values of the first and second users, progressing toward an end of said sequence values (330);

completing (480/483) the exchange provided that the total number of iterations are completed, and terminating (480/490) the exchange if the total number of iterations are not completed.

Support for the elements of claim 23 can be found at least from the following sections of Appellants' specification: [0033]-[0036], [0039], [0044]-[0049], [0052]-[0066] and Figures 3-6.

**Grounds of Rejection to be Reviewed on Appeal**

Claims 1, 3, 4, 6, 7, 9, 10, and 23-25 are rejected under 35 U.S.C. §103(a) as being unpatentable over Asokan et al. (U.S. Publication No. 2002/0049601, hereinafter "Asokan") in view of Micali et al. (U.S. Patent No. 4,944,009, hereinafter "Micali").

## Arguments

### Rejection Under 35 U.S.C. §103

#### Claims 1, 3, 4, 6, 7, 9, and 10

The Examiner has rejected claims 1, 3, 4, 6, 7, 9, and 10 under 35 U.S.C. §103(a) as being unpatentable over Asokan et al. (U.S. Patent Publication No. 2002/0049601, hereinafter "Asokan") in view of Micali et al. (U.S. Patent No. 4,944,009, hereinafter "Micali").

Appellants note that the Advisory Action, dated October 10, 2007 does not address the arguments that Appellants provided in their response to the Final Office Action, dated July 26, 2007, but merely recites the arguments previously provided by the Examiner in the Final Office Action, dated July 26, 2007.

In general, Asokan discloses a method for fair exchange of value items between two parties. According to Asokan's invention, there are two major steps in the value exchange proceedings. First, each party sends a permit that allows the receiving party to confirm the value item, but does not allow extracting the item. Second, if both parties accept the permits as correct, thus binding the representation of the expected values, then the parties send the actual value items to each other (see Abstract).

Asokan, however, fails to teach or suggest Appellants' claim 1 as a whole. Namely, Asokan fails to teach or suggest at least the following elements:

> "iteratively exchanging the sequence values of the first and second users, progressing in a predetermined order toward an end of said sequence values;
>
> completing the exchange provided that the total number of iterations are completed, and terminating the exchange if the total number of iterations are not completed,"

as claimed in independent claim 1. Appellants' claim 1 is directed towards a method providing a "fair" exchange of hidden values that are not revealed at once, but instead, through a process in which the sequence values are iteratively revealed and exchanged, each iteration bringing the two parties closer to the point at which it is possible for both of them to derive the full hidden values of their respective adverse party. Such a process

allows each party to verify repeatedly that the other party is going ahead with the transaction as that party has committed previously, and without placing one party at a significant disadvantage when compared with the other party.

By contrast, Asokan discloses that only ones, at the time the parties exchange/accept permits, does each party verify that the other party is going ahead with the transaction as that party has previously committed. Only ones, the exchange of values takes place. Furthermore, the verification step and exchange of value step of Asokan involve different actions with different purposes. Therefore, neither of the steps or their combination can be interpreted as "iteratively exchanging the sequence values," as claimed in Appelants'independent claim 1.

In the Final Office Action, dated July 26, 2007, the Examiner states that Appellants do not disclose "an iteration of values transferred between users" (Office Action, page 2). Accordingly, Examiner interprets the term "iteration" to be merely a sequence of values (id.). Appellants respectfully disagree.

Though Appellants do not use the word "iteration" in describing their invention, what Appellants do describe includes, in fact, iterative processes. Appellants' invention concerns a "fair" exchange of hidden values that obscure digital certificates or passwords or the like, by a mathematical function such as exclusive-OR or modular multiplication. According to the invention, as disclosed and claimed, the sequence values are revealed and exchanged according to an iterative process, wherein each iteration brings the two parties closer to the point at which it is possible for both of them to derive the full hidden information of their respective adverse party.

For example, Figure 4 represents one of the embodiments of the Appellants' invention. As evidenced from Figure 4 and the paragraphs describing Figure 4, [0044-0049], the time line includes at least two sets of entries of identification markers (sequence values) – a "time line for K entries" (block 420) and a "mirror time line" (block 430). These identification markers are transmitted from a first party to the second (other) party. However, they are not transmitted all together at once, but instead, one by one or in groups (Fig. 4, block 485) until all entries of the time line have been transmitted. (See Fig. 4, element 480). Before each next marker or group of markers could be transmitted to the second party, the first party has to receive a comparable entry

from the second party. As evidenced from Figure 4, steps of blocks 485, 460, 470 and 480 – exchanging of the sequence values between the first and the second party – are repeated until all entries of the time line are transmitted. The cycle repeats because answer "no" to the question of block 480 causes execution of step 485, which is indicated by connection "B" between blocks 480 and 485.

Figure 6 represents another embodiment of the Appellants' invention involving iterative processes similar to those showed in Figure 4. As evidenced from Figure 6 and the paragraphs describing Figure 6, [0057-0058], the cycle of exchanging the sequence values continues until one of the parties stops responding (block 460) or all entries have been transmitted (block 480). Because iteration is a process of repeating, doing something again and again, Appellants do disclose the "iteratively exchanging the sequence values," as recited in claim 1, where the number of entries in the time line represents the total number of iterations required to determine the hidden value without forcing such determination.

Further, a modular function of Appellants' invention iteratively produces a plurality of sequence values. As described in the specification, each such sequence value is related to the next previous sequence value. For an example, the sequence from one value to the next one can be produced via squaring or exponentiation by different number of times (see Para. [0032]). Therefore, because the same action has to be repeated over and over, each such action is accurately characterized as iteration. Also, paragraph [0037] provides an example of formula [6] that could be used to produce the plurality of the sequence values. Because the formula requires repeating its calculations for different "i" values from 0 to K, each of these calculations is iterative. Accordingly, Appellants' element of "iteratively exchanging the sequence values" is fully supported by the specification and does not introduce new matter.

In the Final Office Action, dated July 26, 2007, the Examiner cites specific portions of Asokan (namely, Paras. [0042] and [0043] of Asokan), asserting that the cited portions of Asokan teach Appellants' element of "iteratively exchanging the sequence values of the first and second users, progressing in a predetermined order toward an end of said sequence values." Appellants respectfully disagree.

These paragraphs of Asokan have nothing to do with "iteratively exchanging the

sequence values." Rather, they disclose that information (set of values) used in the encryption process can be requested by one party and stored by another. First, because one party requests but another receives, there is only one party that receives a set of values. This is not exchange, as an exchange requires both parties receiving values. Second, paragraphs [0142] and [0143] do not teach or suggest iterative actions. Paragraph [0143] states that, "P can request several coupons at a time." "At a time" means that all requests are sent during one transaction, not iteratively.

The Appellants' claimed invention is entirely different. As it was discussed above and as it is disclosed in the specification, during the iterations, the first party and second party successively disclose values that lead up to the end of the sequences. Because the parties know the modular functions and the manner of the exchange, during each of the iterations the parties verify that the other party is going ahead as they committed to do, thus verifying numerous times. It is possible for each party to determine whether the other party is in conformance with the rules because the successive high or low end values can be tested for exponentiation according to the modular function. When the entire sequence of exchanges is completed, both parties obtain their adverse party's hidden data. However, should either party renege, neither party is at a substantial disadvantage because both parties have a comparable computing job to complete in order to reach the end of the sequence from the information that each received up to the point that their counterpart reneged. It should be reiterated that, according to Appellants' invention, each party moves towards the hidden value gradually, acquiring the hidden value only through a series of iterations.

The Examiner also cites specific portions of Asokan (namely, Paras. [0072] and [0073] of Asokan), asserting that the cited portions of Asokan teach Appellants' element of "completing the exchange provided that the total number of iterations are completed, and terminating the exchange if the total number of iterations are not completed." Appellants respectfully disagree.

The cited portions merely disclose a procedure of verifying permits of parties participating in exchange. The portions further disclose that if the verification is unsuccessful, the exchange of data between parties is aborted. However, these do not explicitly disclose that the completion of exchange depends on whether "the total number

of iterations are completed," as claimed in independent claim 1. Furthermore, as discussed above, Asokan does not teach or suggest that the exchange of values should or can be accomplished iteratively or how the number of iterations could be chosen or used. Therefore, the cited portions of Asokan simply cannot teach or suggest that the completion of exchange depends on whether "the total number of iterations are completed" and such a dependency is not inherent to Asokan's invention.

Therefore, Appellants respectfully submit that Asokan is devoid of any teaching or suggestion of "iteratively exchanging the sequence values," much less that completing the exchange depends on whether "the total number of iterations are completed."

As such, for at least the above discussed reasons, Asokan fails to teach or suggest at least Appellants' elements of "iteratively exchanging the sequence values of the first and second users, progressing in a predetermined order toward an end of said sequence values" and "completing the exchange provided that the total number of iterations are completed, and terminating the exchange if the total number of iterations are not completed."

Furthermore, Micali, alone or in combination with Asokan, fails to teach or suggest at least the above named elements of Appellants' claim 1.

In contrast to Appellants' claim 1, Micali merely describes a random sequence generator that expands an input sequence to an output sequence substantially greater in length than the input sequence via tree structure (see Abstract). However, Micali does not describe, teach, or suggest "exchanging the sequence values of the first and second users, progressing in a predetermined order toward an end of said sequence values," much less "iteratively exchanging the sequence values of the first and second users, progressing in a predetermined order toward an end of said sequence values," as claimed in Appellants' independent claim 1. Further, the Examiner did not present any arguments that Micali does disclose the above named Appellants' elements.

In the Final Office Action, dated July 26, 2007, the Examiner indicates that Appellants' term "iteration" is interpreted to be merely "a sequence of values such as generated by the Micali prior art" (see Office Action, page 2). The Examiner also states that the random numbers generated by Micali's invention are the plurality of sequence

values of the Appellants' invention because "the random numbers are still in sequence" (see Office Action, page 3). Appellants respectfully disagree.

The Office Action provides a definition of "sequence," which is "a number of things or events arranged in order and connected by being alike in some way" (id.). According to this definition, the random numbers of Micali must be "arranged in order and connected by being alike in some way." However, the purpose of generating random numbers is to receive numbers that appear out of order and not connected.

In contrast, the Appellants' plurality of sequence values is more than a succession of random values. The sequence values are values adhering to a function that enables the receiving party to test (proceeding upwardly and downwardly from the ends of the list toward the center of symmetry or otherwise up to the end of the sequence) that the exchange of values is proceeding according to the agreed function. The Appellants' sequence values demonstrate the continuing participation and good faith of both parties to the transaction. Accordingly, it is inappropriate to equate Appellants' "iteration" or "sequence values" with Micali's random numbers.

The Examiner states that Micali discloses that "difference values between adjacent ones of [the] sequence values are symmetrically distributed about one of [the] values of a known order" (Office Action, page 6). Applicants respectfully disagree.

As described above, Micali simply teaches a random number generator. Micali also discloses that Blum integers could be used to generate random numbers. However, using Blum integers in generating random numbers does not necessarily produce symmetrically distributed sequence values. Nowhere in the cited portions (namely col. 2, lines 43-47 and col. 4, lines 10-13 of Micaly) does Micali discuss such symmetry or reasons for seeking such symmetry. If anything, one of ordinary skill in the art might consider symmetry to be the opposite of random. Because Micali teaches the generation of random numbers, it does not teach or suggest symmetrical distribution of difference values between adjacent sequence values about one of the values of a known order.

Accordingly, because Asokan and Micali each fail to teach or even suggest at least Appellants' elements of "iteratively exchanging the sequence values of the first and second users, progressing in a predetermined order toward an end of said sequence values" and "completing the exchange provided that the total number of iterations are

completed, and terminating the exchange if the total number of iterations are not completed," any permissible combination of Asokan and Micali must also fail to teach or suggest at least these elements of Appellants' independent claim 1.

The test under 35 U.S.C. §103 is not whether an improvement or a use set forth in a patent would have been obvious or non-obvious; rather the test is whether the claimed invention, considered as a whole, would have been obvious. Jones v. Hardy, 110 U.S.P.Q. 1021, 1024 (Fed. Cir. 1984) (emphasis added). Therefore, it is impermissible to focus either on the "gist" or "core" of the invention, Bausch & Lomb, Inc. v. Barnes-hind/Hydrocurve, Inc., 230 U.S.P.Q. 416, 420 (Fed. Cir. 1986) (emphasis added). Moreover, the invention as a whole is not restricted to the specific subject matter claimed, but also embraces its properties and the problems it solves. In re Wright, 6 U.S.P.Q. 2d 1959, 1961 (Fed. Cir. 1988). Asokan and Mecali, alone or in any permissible combination fail to teach or suggest Appellants' independent claim 1, as a whole.

As such, Appellants submit that independent claim 1 is not obvious and fully satisfies the requirements of 35 U.S.C. §103 and is patentable thereunder. Furthermore, claims 3, 4, 6, 7, 9, and 10 depend directly or indirectly from independent claim 1 and recite additional elements thereof. Accordingly, for at least the same reasons as discussed above, Appellants submit that these dependent claims are also non-obvious and fully satisfy the requirements of 35 U.S.C. §103 and are patentable thereunder.

Therefore, Appellants respectfully request that the Examiner's objection be withdrawn.

**Claims 23-25**

The Examiner has rejected claims 23-25 under 35 U.S.C. §103(a) as being unpatentable over Asokan et al. (U.S. Patent Publication No. 2002/0049601, hereinafter "Asokan") in view of Micali et al. (U.S. Patent No. 4,944,009, hereinafter "Micali").

The teachings of Asokan and Micali are discussed hereinabove. For at least the reasons discussed hereinabove with respect to claim 1, Appellants respectfully submit that Asokan and Micali, alone or in combination, fail to teach or suggest Appellants' claim 23 as a whole. Namely, Asokan and Micali fail to teach or suggest at least the elements of "iteratively exchanging the sequence values of the first and second users,

progressing toward an end of said sequence values" and "completing the exchange provided that the total number of iterations are completed, and terminating the exchange if the total number of iterations are not completed," as claimed in Appellants' claim 23.

Accordingly, Appellants submit that independent claim 23 is not obvious and fully satisfies the requirements of 35 U.S.C. §103 and is patentable thereunder. Furthermore, claims 24 and 25 depend directly from independent claim 23 and recite additional elements thereof. Accordingly, for at least the same reasons as discussed above, Appellants submit that these dependent claims are also non-obvious and fully satisfy the requirements of 35 U.S.C. §103 and are patentable thereunder.

Therefore, Appellants respectfully request that the Examiner's objection be withdrawn.

## Conclusion

Therefore, Appellants submit that all of the claims presently in the application are allowable under the provisions of 35 U.S.C. §103.

For the reasons advanced above, Appellants respectfully urge that the rejections of claims 1, 3, 4, 6, 7, 9, 10 and 23-25 are improper. Reversal of the rejections of the Final Office Action is respectfully requested.

Respectfully submitted,

Dated: 12/31/07

Eamon J. Wall
Registration No. 39,414
Patterson & Sheridan, L.L.P.
595 Shrewsbury Ave. Suite 100
Shrewsbury, NJ 07702
Telephone: (732) 530-9404
Facsimile: (732) 530-9808
Attorney for Appellant

## CLAIMS APPENDIX

**LISTING OF CLAIMS:**

Please reconsider the claims as follows:

1. (previously presented) A method fairly exchanging a hidden value of a first user for a hidden value of a second user, by a series of exchanges between the first user and the second user leading up to completing said hidden values, comprising the steps of:

establishing a modulus and a modular function known to the first user and known to the second user, said modular function iteratively producing a plurality of sequence values wherein each said sequence value is related, according to said modular function, to a next previous sequence value, whereby conformance to the modulation function can be determined for adjacent ones of the plurality of sequence values;

establishing a total number of iterations over which the sequence values will be exchanged between the first user and the second user;

iteratively exchanging the sequence values of the first and second users, progressing in a predetermined order toward an end of said sequence values;

completing the exchange provided that the total number of iterations are completed, and terminating the exchange if the total number of iterations are not completed.

2. (canceled)

3. (previously presented) The method of claim 1, wherein said plurality of values are determined according to the modular function by a root value and a modulus value.

4. (previously presented) The method of claim 1, wherein said sequence values are determined over a known order equal to the total number of iterations, wherein each said sequence value is a result of the modular function applied to a next previous sequence value, raised to a power related to a difference in position between said sequence value and a respective beginning and end of the order.

5. (canceled)

6. (previously presented) The method of claim 4, wherein said modulus value is a product of Blum integers.

7. (previously presented) The method of claim 6, wherein said Blum integers comprise prime numbers.

8. (canceled)

9. (previously presented) The method of claim 1, wherein said hidden value is a value immediately preceding a last value of said sequence.

10. (previously presented) The method of claim 1, wherein said number of iterations is at least 80.

11 - 22. (canceled)

23. (previously presented) A system for exchanging user information over a network comprising:

at least one programmed processor coupled to a memory and arranged for conducting a fair exchange of a hidden value of a first user for a hidden value of a second user, by a series of exchanges between the first user and the second user leading up to completing said hidden values;

establishing a modulus and a modular function known to the first user and known to the second user, said modular function iteratively producing a plurality of sequence values wherein each said sequence value is related, according to said modular function, to a next previous sequence value, whereby conformance to the modular function can be determined for adjacent ones of the plurality of sequence values;

establishing a total number of iterations over which the sequence values will be exchanged between the first user and the second user,

iteratively exchanging the sequence values of the first and second users, progressing toward an end of said sequence values;

completing the exchange provided that the total number of iterations are completed, and terminating the exchange if the total number of iterations are not completed.

24. (previously presented) The system of claim 23, further comprising a further processor and wherein said processor and said further processor exchange said sequence values on behalf of the first and second users, respectively.

25. (previously presented) The system of claim 23, wherein said processor is operable to effect the series of exchanges on a timed-basis.

26 - 29. (canceled)

## EVIDENCE APPENDIX

None

## RELATED PROCEEDINGS APPENDIX

None